



## [12] 发明专利申请公开说明书

[21] 申请号 01134408.3

[43] 公开日 2003 年 5 月 7 日

[11] 公开号 CN 1416239A

[22] 申请日 2001.10.31 [21] 申请号 01134408.3

[71] 申请人 华为技术有限公司

地址 518057 广东省深圳市科技园科发路华为用服大厦

[72] 发明人 袁松 李安

[74] 专利代理机构 北京德琦专利代理有限公司

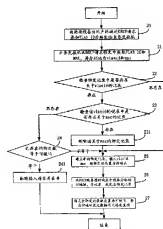
代理人 王丽琴

权利要求书 3 页 说明书 11 页 附图 3 页

[54] 发明名称 光纤同轴混合接入网中的虚拟局域网接入方法

## [57] 摘要

本发明涉及一种 HFC 接入网中的 VLAN 接入方法，通过采用 VLAN ID + MAC 地址 + IP 地址绑定的方式来识别每个终端设备 (CM) 下的每个用户终端，提高系统接入的精确性、安全性与可管理性。其用户报文标识设置过程是：由接入层局端设备为用户终端发出的 DHCP 请求报文添加 VLAN ID；由分发层业务交换机提取 VLAN ID 和 MAC 地址，并记录在端口数据表中；由 DHCP 服务器为 DHCP 请求分配 IP 地址；由分发层业务交换机在端口数据表中建立 VLAN ID、MAC 地址、IP 地址的绑定记录项。数据报文处理过程是：由分发层业务交换机从数据报文中提取 VLANID、MAC 地址和 IP 地址；与端口数据表中绑定记录项中的任意一个绑定记录比较；对符合或不符合任意一个绑定记录的数据报文分别进行丢弃或转发处理。



1. 一种光纤同轴混合 (HFC) 接入网中的虚拟局域网 (VLAN) 接入方法, 由接入层局端设备 (CMTS) 和终端设备 (CM) 提供光纤同轴混合 (HFC) 接入和由分发层业务交换机对终端设备 (CM) 下并发接入的用户终端进行识别, 包括
- 5 用户报文标识设置处理过程和数据报文处理过程, 其特征在于:

所述的用户报文标识设置处理过程包括以下步骤:

- A. 由接入层局端设备 (CMTS) 为用户终端发出的动态主机配置协议 (DHCP) 请求报文添加虚拟局域网标识 (VLAN ID) 后转发至分发层业务交换机;
- B. 分发层业务交换机从动态主机配置协议 (DHCP) 请求报文中提取虚拟局
- 10 域网标识 (VLAN ID) 和介质访问控制 (MAC) 地址, 并记录在端口数据表中;
- C. 由动态主机配置协议 (DHCP) 服务器按指定的规则为该动态主机配置协议 (DHCP) 请求报文分配互联网协议 (IP) 地址, 并在动态主机配置协议 (DHCP) 响应中返回给分发层业务交换机;
- D. 由分发层业务交换机在端口数据表中建立起虚拟局域网标识 (VLAN ID)
- 15 与介质访问控制 (MAC) 地址、互联网协议 (IP) 地址的绑定记录项;

所述的数据报文处理过程包括以下处理步骤:

- E. 从端口接收到数据报文的分发层业务交换机, 从数据报文中提取虚拟局域网标识 (VLAN ID)、介质访问控制 (MAC) 地址和互联网协议 (IP) 地址;
- F. 分发层业务交换机检查该端口数据表中的绑定记录项, 判定提取的虚拟
- 20 局域网标识 (VLAN ID)、介质访问控制 (MAC) 地址和互联网协议 (IP) 地址是否符合端口数据表中绑定记录项中的任意一个绑定记录;
- G. 转发符合任意一个绑定记录的数据报文或丢弃不符合任意一个绑定记录的数据报文。

2. 根据权利要求1所述的一种光纤同轴混合 (HFC) 接入网中的虚拟局域网 (VLAN) 接入方法, 其特征在于: 所述的虚拟局域网标识 (VLAN ID) 是接入层
- 25 局端设备 (CMTS) 分配给特定终端设备 (CM) 下所有用户终端的虚拟局域网 (VLAN)

标识;所述的介质访问控制(MAC)地址是接入用户终端的介质访问控制(MAC)地址,所述的互联网协议(IP)地址是动态主机配置协议(DHCP)服务器通过动态主机配置协议(DHCP)分配给接入用户终端的互联网协议(IP)地址。

3. 根据权利要求1所述的一种光纤同轴混合(HFC)接入网中的虚拟局域网(VLAN)接入方法,其特征在于:所述的步骤B进一步包括:

b1. 分发层业务交换机从业务端口接收到动态主机配置协议(DHCP)请求报文,从采用以太网帧格式的报文头中提取虚拟局域网标识(VLAN ID)和介质访问控制(MAC)地址,并分别记为vlanid和mac;

- b2. 检查数据表的绑定记录项中是否存在关于vlanid的绑定记录,当关于vlanid的绑定记录数等于0时执行步骤C,在关于vlanid的绑定记录数大于或等于1时,执行步骤b3;

b3. 在该关于vlanid的绑定记录中,检查是否存在关于mac的绑定记录,当存在关于mac的绑定记录时,删除该关于mac的绑定记录,然后执行步骤C,当不存在关于mac的绑定记录时,执行步骤b4;

- b4. 进一步判定关于vlanid的绑定记录中已经存在的绑定记录数是否等于预设的阈值,当等于预设的阈值时,拒绝所述的动态主机配置协议(DHCP)请求并丢弃数据报文,当小于预设的阈值时,继续执行步骤b5;

b5. 在数据表中建立一条新的绑定记录项,将步骤b1中记录的vlanid和mac填写到该绑定记录项中,并将其绑定状态置为待确认;

- 所述的步骤D进一步包括:

d1. 分发层业务交换机从响应报文中提取所述的互联网协议(IP)地址,并将IP地址填写到由步骤b5建立的待确认绑定记录项中,形成完全绑定记录项;

d2. 将新建立的完全绑定记录项的状态置为可使用状态,并为记录中的互联网协议(IP)地址设定数据报文转发表项。

4. 根据权利要求3所述的一种光纤同轴混合(HFC)接入网中的虚拟局域网(VLAN)接入方法,其特征在于:所述步骤b4中的阈值是同一个终端设备(CM)

下并发接入的用户终端的数目，也即允许分配给同一个终端设备（CM）下用户终端的互联网协议（IP）地址的数目。

5. 根据权利要求3或4所述的一种光纤同轴混合（HFC）接入网中的虚拟局域网（VLAN）接入方法，其特征在于：所述的阈值大于1。

- 5       6. 根据权利要求1所述的一种光纤同轴混合（HFC）接入网中的虚拟局域网（VLAN）接入方法，其特征在于所述的步骤C还包括：判断终端设备（CM）是否申请过并发接入业务，对于没有申请过并发接入业务的终端设备（CM）下的用户终端只给予分配一个互联网协议（IP）地址；对于申请过并发接入业务的终端设备（CM）下的用户终端给予分配等于阈值的互联网协议（IP）地址。
- 10       7. 根据权利要求1所述的一种光纤同轴混合（HFC）接入网中的虚拟局域网（VLAN）接入方法，其特征在于所述步骤F中的“判定”与“符合”是：从接收的数据报文中提取的虚拟局域网标识（VLAN ID）必须是数据表绑定记录中的虚拟局域网标识（VLAN ID）；从接收的数据报文中提取的介质访问控制（MAC）地址必须是数据表绑定记录中的介质访问控制（MAC）地址；从接收的数据报文中提取的互联网协议（IP）地址必须是数据表绑定记录中的互联网协议（IP）地址。
- 15

## 光纤同轴混合接入网中的虚拟局域网接入方法

### 技术领域

本发明涉及接入网技术领域，更确切地说是涉及一种采用虚拟局域网（VLAN）接入方式的光纤同轴混合接入网（HFC）的接入方法。

### 背景技术

所谓接入网是业务提供点与最终用户之间的连接网络。在现有的接入网中，业务交换机可以通过多种介质接入数据业务，其中包括非对称数字用户线（ADSL）、光纤同轴混合网（HFC）和以太网。

所谓 HFC 接入网，大都是采用 DOCSIS 或 EuroDOCSIS 协议在 HFC 双向网上实现的上、下行非对称的接入网。HFC 接入方式借助于带宽可以实现 750M/860M 的有线电视网络，开展宽带接入业务，具有带宽宽、永远在线、一线入户、网络现成的优点。广电网络因为拥有现成的遍布千家万户的 HFC 网络而成为许多投资商投资的对象。在建立 HFC 接入网络方面，目前的现状是由用户直接接入，由于在接入中没有进行认证，因而安全性差，网络不好运营也不好管理。

一般来讲，HFC 有两种接入方式可供选择：点对点协议（PPP，本发明不讨论 PPP 接入方式）接入方式和虚拟局域网（VLAN）接入方式。其中，VLAN 接入方式是建立在局域网交换机硬件基础上的、通过软件可以进行配置和管理、划分逻辑工作组的方法。

HFC 系统中 VLAN 的划分方式有多种，常用的有两种：按照介质访问控制（MAC）地址划分的 VLAN 和按照用户终端（CM）划分的 VLAN。本发明涉及的是按用户终端（CM）划分的 VLAN。为了使网络可管理、可运营，无论网络服务提供商选择何种方式接入用户，业务交换机都应该提供完善的用户

管理手段，如：准确的识别用户、禁止/允许特定用户的接入、防止地址仿冒、阻断恶意攻击、用户优先级保证、计费等等。其中，对用户的识别是实现其他功能的前提。

本发明具体涉及的就是在 HFC 接入网上，采用 VLAN 接入方式时，业务  
5 交换机对用户的识别方法。

参见图1，图中示出现有技术中，HFC接入网VLAN接入方式的组网结构，是采用以接入层设备+分发层设备方式接入时的组网结构。组网结构中包括用户终端（CPE、IDT智能终端等）、HFC接入网、网管服务器（NMS，包括DHCP SERVER、TFTP SERVER、TOD SERVER、网管系统）以及用于完成授权、验证和计费功能的  
10 AAA服务器等。

其中，HFC接入网一般划分为两个层次：L2接入层和L2/L3分发层。L2接入层包括局端设备CMTS（如图中的MA5201）和终端设备CM，CMTS和CM之间通过HFC双向网相连接，CM通过5类双绞线与用户终端CPE或IDT智能终端设备直接相连，L2接入层主要完成汇聚功能，用户终端设备通过CM接入到HFC系统。L2接入层和  
15 L2/L3分发层一般通过5类线相连。

L2/L3分发层主要完成业务汇聚、L2/L3分发等功能。用户通过HFC系统的L2接入层接入到分发层设备，L2/L3分发层采用L3交换机或者业务交换机（如图中的MA5200）。其中采用业务交换机是今后的发展方向，在分发层中采用业务交换机，可以完成多业务转发、验证/计费、虚拟专网（VPN）等多种功能，可  
20 有效地提高骨干网络的使用效率。图中局端设备CMTS与业务交换机间的FE是两个以太网交换机的接口。

当采用VLAN接入方式时，通常将接入层每个CM下的用户划分到不同的VLAN中，利用VLAN的分隔功能，使用户之间不能互相访问。业务交换机利用虚拟局域网标识（VLAN ID），可以判定一个业务报文是从哪个CM发来的。

25 如在业务交换机（MA5201）上通过命令行终端（CLI）或网管工作站（NMS）配置本业务交换机（MA5201）设备需要的VLAN ID、该业务交换机（MA5201）设

备下所有CM的共享VLAN ID。CM的启动配置文件在NMS上生成，接入CM的CPE、IDT智能终端所使用的VLAN ID在NMS生成配置文件时指定。接入一个CM的所有设备共用一个VLAN ID，这些设备的所有上行报文中的VLAN ID，都在CMTS局端设备（MA5201）上添加生成。这样业务交换机（MA5200）接收到的每个数据报文都  
5 包含VLAN ID。由于VLAN ID是按照特定的规则分配的，这样业务交换机（MA5200）就可以根据数据报文中的VLAN ID判断出报文的来源，判断结果精确到特定的CM。

图1中示出的实例是由接入层设备（CMTS局端设备MA5201）提供HFC接入，（业务交换机MA5201）通过识别数据报文的VLAN ID进行用户接入控制。采用该  
10 CMTS局端设备（MA5201）+业务交换机（MA5200）的组合方式接入，可提供灵活的组网能力和强大的运营管理维护功能。

对于VLAN接入方式，用户的概念包含两个层次：第一层是终端设备（CM）；第二层是终端设备（CM）下接入的计算机。如果每个CM下只接入一台用户计算机，那么一个CM与接入的一台用户计算机是一一对应的，使用第一层（CM）的  
15 VLAN ID就可以唯一地标识出第二层的该计算机。在这种情况下，把VLAN ID作为运营商分配给用户的唯一标识是可行的，这也是目前大多数接入设备的典型做法。

但是，当一个CM通过集线器（HUB）连接了多台用户计算机时，一VLAN ID与多个用户计算机之间形成一对多的关系，在这种情况下，如果接入层设备还是简单地利用VLAN ID来标识用户，由于这种方法只能精确到CM，要想准确判定  
20 数据报文来自同一CM下的哪台计算机就无能为力了。

每个CM最多可接入的用户数量是可以配置在接入层设备（MA5201）的网管服务器（NMS）上的，而在实际应用情况中，也是每户设置一个CM，在一个CM下接入多个CPE时，由于计费是由这个家庭（CM）总支付的，因此对用户计算机  
25 识别到CM是没有什么问题的。如图中所示的在一户住宅里，通过智能终端IDT

连接多个设置有各种传感器(水、气、电等)的数字计量装置,通过集线器(HUB)连接用户计算机(CPE),IDT、CPE通过一个CM接入HFC。

如果一个CM下带有多个CPE用户、IDT智能终端,由于上面所述的方法只能精确判断到单个的CM,要想准确识别数据报文来自哪台计算机就不可能了。

- 5 综上所述,由于一个CM下的各计算机被认为是相同的用户,传统的方法是针对每台CM进行准确与详尽的统计,不可能向一个CM下的每个计算机用户都提供详细的使用清单;而在特定的情况下,用户会关心每台计算机的使用情况,因而要求能够识别到用户计算机,就可以按照计算机来统计相关的信息了。

#### 10 发明内容

本发明的目的是设计一种光纤同轴混合(HFC)接入网中的虚拟局域网(VLAN)接入方法,针对现有技术中分分层设备只能识别到CM的情况作出改进设计,使分分层设备可以管理到每个CM下的每台计算机。

- 15 在采用接入层设备加分发层设备(如MA5201+MA5200)方式组网时,本发明采用以虚拟局域网标识(VLAN ID)+介质访问控制(MAC)地址+互联网协议(IP)地址绑定的方法来识别每个终端设备(CM)下的每个终端用户,使分发层(MA5200)设备在以VLAN接入方式组网运行时,可以精确地辨别数据报文来源,从而实现以用户计算机为对象的用户管理。

- 20 本发明的一种光纤同轴混合(HFC)接入网中的虚拟局域网(VLAN)接入方法,应用在采用接入层局端设备(CMTS)与终端设备(CM)加分发层业务交换机组网方式的光纤同轴混合(HFC)接入网的网络中,所述网络还包括网管服务器(NMS)和用于授权、验证与计费的AAA服务器,终端设备(CM)下有一台以上的用户终端并发接入。

- 25 实现本发明目的的技术方案是这样的:一种光纤同轴混合(HFC)接入网中的虚拟局域网(VLAN)接入方法,由接入层局端设备(CMTS)和终端设备(CM)提供光纤同轴混合(HFC)接入和由分发层业务交换机对终端设备(CM)下并发



接入的用户终端进行识别,包括用户报文标识设置处理过程和数据报文处理过程,其特征在于:

所述的用户报文标识设置处理过程包括以下步骤:

- A. 由接入层局端设备(CMTS)为用户终端发出的动态主机配置协议(DHCP)  
5 请求报文添加虚拟局域网标识(VLAN ID)后转发至分发层业务交换机;

B. 分发层业务交换机从动态主机配置协议(DHCP)请求报文中提取虚拟局域网标识(VLAN ID)和介质访问控制(MAC)地址,并记录在端口数据表中;

C. 由动态主机配置协议(DHCP)服务器按指定的规则为该动态主机配置协议(DHCP)请求报文分配互联网协议(IP)地址,并在动态主机配置协议(DHCP)

- 10 响应中返回给分发层业务交换机;

D. 由分发层业务交换机在端口数据表中建立起虚拟局域网标识(VLAN ID)与介质访问控制(MAC)地址、互联网协议(IP)地址的绑定记录项;

所述的数据报文处理过程包括以下处理步骤:

- E. 从端口接收到数据报文的分发层业务交换机,从数据报文中提取虚拟局  
15 域网标识(VLAN ID)、介质访问控制(MAC)地址和互联网协议(IP)地址;

F. 分发层业务交换机检查该端口数据表中的绑定记录项,判定提取的虚拟局域网标识(VLAN ID)、介质访问控制(MAC)地址和互联网协议(IP)地址是否符合端口数据表中绑定记录项中的任意一个绑定记录;

- G. 转发符合任意一个绑定记录的数据报文或丢弃不符合任意一个绑定记录  
20 的数据报文。

所述的虚拟局域网标识(VLAN ID)是接入层局端设备(CMTS)分配给特定终端设备(CM)下所有用户终端的虚拟局域网(VLAN)标识;所述的介质访问控制(MAC)地址是接入用户终端的介质访问控制(MAC)地址,所述的互联网协议(IP)地址是动态主机配置协议(DHCP)服务器通过动态主机配置协议(DHCP)

- 25 分配给接入用户终端的互联网协议(IP)地址。

所述的步骤B进一步包括:

b1. 分发层业务交换机从业务端口接收到动态主机配置协议 (DHCP) 请求报文, 从采用以太网帧格式的报文中提取虚拟局域网标识 (VLAN ID) 和介质访问控制 (MAC) 地址, 并分别记为vlanid和mac;

b2. 检查数据表的绑定记录项中是否存在关于vlanid的绑定记录, 当关于  
5 vlanid的绑定记录数等于0时执行步骤C, 在关于vlanid的绑定记录数大于或等于1时, 执行步骤b3;

b3. 在该关于vlanid的绑定记录中, 检查是否存在关于mac的绑定记录, 当存在关于mac的绑定记录时, 删除该关于mac的绑定记录, 然后执行步骤C, 当不存在关于mac的绑定记录时, 执行步骤b4;

10 b4. 进一步判定关于vlanid的绑定记录中已经存在的绑定记录数是否等于预设的阈值, 当等于预设的阈值时, 拒绝所述的动态主机配置协议 (DHCP) 请求并丢弃数据报文, 当小于预设的阈值时, 继续执行步骤b5;

b5. 在数据表中建立一条新的绑定记录项, 将步骤b1中记录的vlanid和mac填写到该绑定记录项中, 并将其绑定状态置为待确认;

15 所述的步骤D进一步包括:

d1. 分发层业务交换机从响应报文中提取所述的互联网协议 (IP) 地址, 并将IP地址填写到由步骤b5建立的待确认绑定记录项中, 形成完全绑定记录项;

d2. 将新建立的完全绑定记录项的状态置为可使用状态, 并为记录中的互联网协议 (IP) 地址设定数据报文转发表项。

20 所述步骤b4中的阈值是同一个终端设备 (CM) 下并发接入的用户终端的数目, 也即允许分配给同一个终端设备 (CM) 下用户终端的互联网协议 (IP) 地址的数目。

所述的阈值大于1。

所述的步骤C还包括: 判断终端设备 (CM) 是否申请过并发接入业务, 对于  
25 没有申请过并发接入业务的终端设备 (CM) 下的用户终端只给予分配一个互联

网协议 (IP) 地址; 对于申请过并发接入业务的终端设备 (CM) 下的用户终端给予分配等于阈值的互联网协议 (IP) 地址。

所述步骤F中的“判定”与“符合”是: 从接收的数据报文中提取的虚拟局域网标识 (VLAN ID) 必须是数据表绑定记录中的虚拟局域网标识 (VLAN ID);

- 5 从接收的数据报文中提取的介质访问控制 (MAC) 地址必须是数据表绑定记录中的介质访问控制 (MAC) 地址; 从接收的数据报文中提取的互联网协议 (IP) 地址必须是数据表绑定记录中的互联网协议 (IP) 地址。

本发明的方法是在包括HFC接入网的网络中实现的。本发明的特征在于: 业务交换机通过虚拟局域网标识 (VLAN ID) + 介质访问控制 (MAC) 地址 + 互联网  
10 协议 (IP) 地址绑定的方法来识别每个CM下的每个用户终端; 其中的VLAN ID是指分配给特定CM下所有用户终端的VLAN的标识, MAC地址是指接入用户终端的MAC地址; IP地址是指由DHCP服务器通过DHCP协议分配给接入用户终端的IP地址。

所谓VLAN ID+MAC地址+IP地址绑定的含义是: 每一个接收到的IP报文, 其  
15 以太网封装帧头中的VLAN ID必须是数据表绑定记录中的VLAN ID; 其以太网封装帧头中的源MAC地址也必须是数据表绑定记录中的MAC地址; 同时此报文的源IP地址也必须是绑定记录中的IP地址。如果不符合上述约束条件, 该报文被视为无效并被丢弃。

实施本发明的HFC接入网中的VLAN接入方法, 由于采用了VLAN ID+MAC地址  
20 +IP地址绑定的方式来识别每个CM下的每个用户终端, 其用户标识的设置可以准确到终端设备 (CM) 下的每一用户终端 (用户计算机), 提高了系统接入的精确性、安全性和可管理性。这样就可以控制并发接入用户终端的数量。

#### 附图说明

图 1 是现有技术中光纤同轴混合网 (HFC) 接入网虚拟局域网 (VLAN)  
25 接入方式的组网结构示意图。

图 2 是本发明方法的用户报文标识设置处理流程框图。

图3是本发明方法的数据报文处理流程框图。

### 具体实施方式

参见图2并结合参见图1,本发明的方法应用于如图1所示的网络结构中,该网络包括用户终端(CPE、IDT)、终端设备(CM)、HFC接入网、网管服务器(NMS, 5 包括DHCP SERVER、TFTP SERVER、TOD SERVER及网管系统)以及用于完成授权、验证与计费功能的AAA服务器。其中,HFC接入网包括L2接入层和L2/L3分发层,L2接入层中采用CMTS局端设备(如MA5201)和终端设备(CM),且一个终端设备(CM)下可以有多台用户终端(CPE、IDT);L2/L3分发层采用业务交换机(如MA5200)。

10 假设一用户计算机的CM已经在局端设备上成功注册,当该用户计算机开机时,首先要经过CM并在局端设备(MA5201)上添加VLAN ID,然后向业务交换机(MA5200)发出动态主机配置协议(DHCP)请求;业务交换机(MA5200)从DHCP请求报文中提取MAC地址和VLAN ID,并记录在端口数据表中,然后将请求转发(Relay)到相应的DHCP服务器(可以将不同种类的CM、CPE、IDT设备发出的DHCP请求报文发往不同的DHCP服务器),以获取IP地址;DHCP服务器按照指定的规则给该用户计算机分配IP地址,并在DHCP响应中向业务交换机(MA5200) 15 返回分配的IP地址;业务交换机(MA5200)收到该响应后,在上述端口数据表中建立一项VLAN ID->MAC->IP的绑定记录。

绑定的含义是:在业务交换机(MA5200)每收到一个来自用户计算机的IP 20 报文时,该报文封装中的VLAN ID必须是数据表绑定记录中的VLAN ID;该报文封装中的源MAC地址也必须是数据表绑定记录中的MAC地址;同时该报文封装中的源IP地址也必须是数据表绑定记录中的IP地址,如果不符合这些约束条件,则该接收的报文就被视为无效报文并被丢弃。

本发明中,每个终端设备(CM)在开户时要注明其使用方式,其中很重要 25 的一点就是是否允许多客户接入以及一个终端设备(CM)端口下能够同时连接的用户终端数,即同时能占用的IP地址数。如果终端设备申请了多客户接入,

在分发层的业务交换机中，还要给每个终端设备（同一VLAN ID）设置一个可供分配的IP地址数目的阈值；如果终端设备设有申请多客户接入，在分发层的业务交换机中，可分配给该终端设备的IP地址数目就为1。

参见图2，是用户报文标识设置处理流程。执行该流程的前提是终端设备（CM）预先申请了并发接入，若终端设备（CM）没有申请并发接入，则该终端设备（CM）下的用户计算机将无法获得IP地址；此外，若该终端设备（CM）虽然申请了并发接入，但该终端设备（CM）已经达到所申请的并发接入的上限（阈值），则该终端设备（CM）下的用户计算机也无法获得IP地址。

步骤20，用户计算机开机后发出动态主机配置协议（DHCP）请求，该请求经过CM并由局端设备添加VLAN ID后转发给业务交换机；

步骤21，业务交换机从业务端口接收到DHCP请求，从DHCP请求的报文头（采用以太网帧格式）中提取VLAN ID和源MAC地址，并分别记为vlanid和mac；

步骤22，检查绑定记录表中是否存在关于vlanid的记录，如果不存在关于vlanid的记录，即记录数等于0，则表明该DHCP请求是来自该CM下首次开机的一用户计算机，进入步骤25处理，如果存在关于vlanid的记录，即记录数大于或等于1，表明该DHCP请求是来自该CM下另一个不是首次开机的用户计算机，则继续执行步骤23；

步骤23，在该关于vlanid的绑定记录中，检查是否存在关于mac的绑定记录，如果存在关于mac的绑定记录，则删除该关于mac的绑定记录（步骤231），然后执行步骤25，如果在关于vlanid的绑定记录中不存在关于mac的绑定记录，则执行步骤24；

步骤24，进一步判定关于vlanid的绑定记录中已经存在的绑定记录数是否等于预设的阈值，如果相等，表示可供分配的用户终端的IP地址数目已达到（等于）上限，应拒绝用户的接入请求并丢弃数据报文（步骤241），如果关于vlanid的绑定记录中已经存在的绑定记录数小于预设的阈值，说明还有可供分配的用户终端的IP地址（可分配的IP地址数目小于阈值），则继续执行步骤25；

步骤25, 在绑定记录中建立一条新的绑定记录, 将步骤21中记录的vlanid和mac填写到记录中, 此时的绑定记录称为待确认绑定记录;

- 步骤26, 业务交换机向DHCP服务器转发DHCP请求, 并等待响应, 在业务交换机收到响应后, 从响应报文中提取由DHCP服务器分配给该用户终端的IP地址,
- 5 并将此IP地址填写到已建立的待确认绑定记录中, 此时的绑定记录称为完全绑定记录;

步骤27, 将新建立的完全绑定记录的状态置为可使用状态, 并为记录中的IP地址设定数据报文转发表项。

- 通过上述步骤可以控制一终端设备 (CM) 下并发接入用户计算机的数量。
- 10 下表中所示为业务交换机上绑定记录的表格示例, 由VLAN ID、源MAC地址、源IP地址和绑定状态各项组成。假定一终端设备 (CM) 申请的并发接入用户的数量为2, 表格中VLAN ID各为2、9的两个绑定记录项, 有不同的源MAC地址, 分配了不同的源IP地址, 绑定记录的状态为可使用状态; 表格中VLAN ID为1的绑定记录, 记录有源MAC地址, 分配了一个源IP地址, 绑定记录的状态为待确认。

VLAN ID	MAC地址	IP地址	绑定的状态
1	ff. 63. 75. 00. 21. 83	10. 110. 0. 1	待确认
2	00. 12. 66. 00. 78. 99	10. 110. 0. 2	待确认
2	33. 34. 67. 82. 11. 59	10. 110. 0. 3	可用
3	x. x. x. x. x. x	x. x. x. x	
...			
8	x. x. x. x. x. x	x. x. x. x	
9	21. 63. 75. 00. 21. 54	10. 110. 0. 111	待确认
9	70. 63. 75. 00. 21. 37	10. 110. 0. 112	可用

15

参见图3, 为本发明方法的数据报文处理流程。

步骤31, 业务交换机的业务端口接收到数据报文;

步骤32, 从接收的数据报文中提取VLAN ID、源MAC地址和源IP地址;

步骤33, 检查绑定记录表, 提取的VLAN ID、源MAC地址和源IP地址是否符合绑定记录中对应终端设备(CM)的任意一个绑定;

步骤34, 如果符合任何一个绑定记录则转发该数据报文;

- 5      步骤35, 如果不符合任何一个绑定记录则判定为无效数据报文, 并丢弃该数据报文。

通过本发明的方法, 业务交换机就能够准确地掌握当前HFC接入网系统已经接入的用户计算机、每台用户计算机所处的终端设备(CM), 以及它的IP地址和MAC地址。有了这些信息, 业务交换机可以记录每台计算机的活动, 控制IP  
10      地址的分配, 限制一终端设备(CM)端口下可接入用户计算机的数量, 并阻断  
    恶意用户对系统的攻击。

本发明的方法可以应用在HFC接入产品中, 在以VLAN方式接入用户业务时, 通过VLAN ID+MAC+IP绑定的方式, 能够精确地识别每个业务端口下接入的用户计算机, 提升了设备的安全性和可管理性。

15

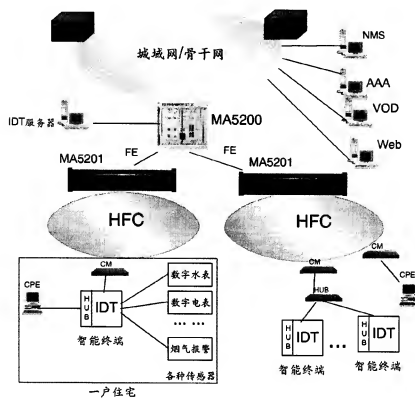


图 1



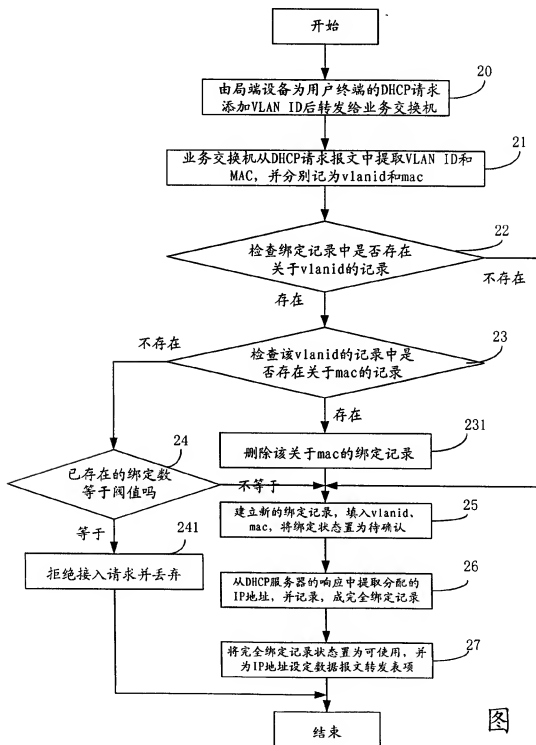


图 2

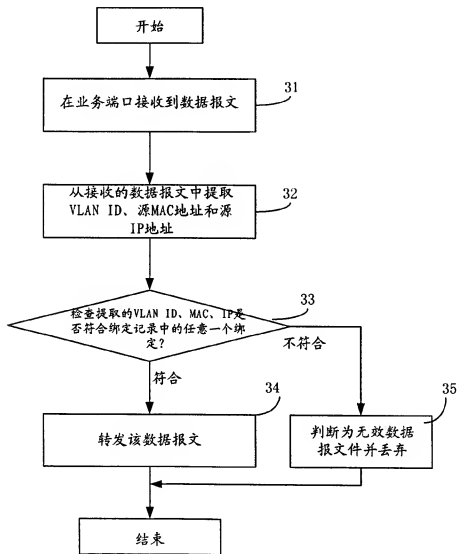


图 3